The program is an implementation of AES encryption which is symmetric key cryptography system.

How to Run?
On the terminal type

python Assignment3.py

INPUT:
Plaintext(of length 16 including spaces)
Key(of length 16 including spaces)

OUTPUT:
Ciphertext in the hexadecimal format

Explanation of the program:
The program is a standard implementation of Advanced Encryption Standard(AES) with a slight variation that it carries out round zero and round one only instead of ten rounds in standard implementation.

There is a fixed matrix(named fixed_matrix) which we use in one of the below mentioned steps.

At first, we convert the given plaintext and key to a 16 byte(4x4 matrix) format with each column representing a word. We call the matrix generated by plaintext as State_matrix which would represent the state of a plaintext as we go through multiple steps in round 0 and round 1.
We call the matrix generated by key as key_matrix.

Round 0: It performs element wise XOR operation on the state_matrix and key_matrix elements.

Round 1: This is represented by round_computation function in the program. There are several steps in this function.

- **Byte_substitution:** This function performs the substitution of the state_matrix elements from the S_Box used for AES. It uses first four bits of the state_matrix element to find the row and the later 4 bits of the state_matrix element to find the column of the S_box. This way we substitute the state matrix element by the element at the (row,column) index at the S_Box matrix.
- **Shift_rows:** This function performs the substitution of the row elements of the state matrix in a cyclic manner as we do in standard implementation of AES.
- **Mix_Coloumns:** This function implements the product of fixed_matrix and state_matrix where addition is replaced by XOR operation and multiplication replaced by multplication over GF(2^8). This is implemented in the function mix_coloumns().
- **Add_round_key(Key expansion):** It is implementing the key expansion and then multiplying the state_matrix and the updated key matrix. As we do in standard version,

the words of the key_matrix and applying the same cyclic shift rows and then taking XOR.

This is continued for each round if the number of rounds performed are more than 1. Here we only show one round with byte substituition scheme, shift rows, mix coloumns and key expansion.

Note that if the input is of any length then we can divide into blocks of 16 characters and then perform the AES encryption.